College of Information & Computer Sciences
University of Massachusetts, Amherst

Project Proposal: Relaxed Authentication in Performance Constrained Networking

Background: Authentication schemes are often too heavyweight to be deployed in authenticated versions of major networking protocols like BGPSec (Secured version of Border Gateway Protocol), which is a security extension of the Border Gateway Protocol and Network Time Security, which enables users to obtain time from the clock synchronization protocol called Network Time Protocol in an authenticated manner.

Relaxing the security notions through *moderate-unforgeability* over the standard unforgeable schemes provides us a way to flexibly tune the probability of forgery attempts being successful, which are produced within computational-resource-constrained higher-level protocols.

The new constructions on message authentication code and digital signature will achieve same practical security and efficiency but with less computational resources. This project will allow us an in-depth look into what security we should aim to achieve, when perfect security (probability of attacker's success being infinitesimally small) is not accomplishable.

Objectives: The aim of this project is to formally introduce the concepts of moderately unforgeable authentication schemes: α-unforgeable message authentication code and α-unforgeable digital signature. The case of digital signatures being the non-trivial one because of attacker's ability to make unbounded number of verification queries in parallel.

Because of their efficient parallelizable operations, lattice-based LWE (Learning with Errors) problem will be investigated to see if security of message authentication code can be scaled down by decreasing the number of samples the adversary receives from an oracle. The problem of scaling down digital signature is resonant with solving subsequent SIS (Short Integer Solution) instances with different random targets. Truncated hash-based signatures are taken into consideration too.

We want to explore the efficiency of α-unforgeable message authentication code with respect to standard blockciphers like AES (Advanced Encryption Scheme), and the efficiency of α-unforgeable digital signature with respect to standard digital signature algorithms like RSA and ECDSA (Elliptic Curve Digital Signature Algorithm). In applications, performance often triumphs over security in trade-offs related to networking protocols. Moderate-unforgeability provides a way to incorporate meaningful security within the bounds of the performance constraints.

Network Time Protocol (NTP) is used for clock synchronization between computer systems over variable-latency data networks. However, NTP is severely resource constrained and cannot use standard message authentication codes. Almost all the attacks on NTP require the adversary to forge a stream of packets over time. The NTP can be adapted and modified to moderately-unforgeable authentication.

Border Gateway Protocol is used to exchange routing and reachability info among autonomous systems on Internet. It's secured counterpart, BGPSec has been adopted at a slow pace because of its resource constraints. Currently, routers use ineffective non-cryptographic solutions like prefix-filtering. BGPSec can be adopted with moderate-unforgeable authentication. We can use chained-nonces [receiver could have a threshold of how many packets late in the chain a given packet could be received, based on the security of the signature scheme] or randomness beacon [receiver could have a time-out threshold for a given packet to be received] to bootstrap moderately-unforgeable signatures depending on the frequency of route announcements.

We also want to explore a low-cost hardware acceleration mechanism that would significantly increase unforgeability. E.g., there can be some operations done by circuits that can be costly to replicate in code. Another direction, for the proposed α-unforgeable schemes is to see if custom FPGA hardware or GPU acceleration could provide a viable attack approach (at a basic level, this might just establish some parameters for the robustness of the unforgeability that is needed beyond overcoming CPU based attacks). The factors like key sizes; complexity of key generation, signer and verifier algorithms; processor clock cycles and time granularity; memory usage; entropy of messages; vulnerability to known attacks; flexibility of application to different platform types; power consumption; these all can affect the security of the schemes and the probability of a successful attack. We plan to evaluate which metrics are relevant and to what extent.

For lattice-based schemes, we can look at a range of row sizes, to see if there is a sweet spot where parallelism best amortizes overhead. For different acceleration mechanisms, GPU and CPU vector extensions; with different overhead, there can be different sizes that are optimal. The smallest that achieves the desired α-unforgeability might not be the most efficient (or might only be most efficient without acceleration). We plan to study the effect of these parameters in detail.

Scope and Timeframe:

Fall 2020 – CS 701Y		
	Description of Work	Start and End Dates
Phase One	Constructions of α-unforgeability for the message authentication codes and digital signatures	24th Aug, 2020 to 14th Sep, 2020 (3 weeks)
Phase Two	Exploration of the metrics affecting the security of the constructions	14th Sep, 2020 to 28th Sep, 2020 (2 weeks)
Phase Three	Development of hardware acceleration techniques for the constructions proposed	28th Sep, 2020 to 9th Nov, 2020 (6 weeks)
Phase Four	Analysis of security and performance of the constructions	9th Nov, 2020 to 30th Nov 2020 (3 weeks)
Spring 2021 – CS 701Y		
Phase Five	Simplify key management needed in Network Time Security with our notion of moderately weak signatures	19th Jan, 2021 to 23th Feb, 2021 (5 weeks)
Phase Six	Analysis of security and performance of the Network Time Security with the moderately unforgeable schemes replacing the standard authentication schemes	23th Feb, 2021 to 23th Mar, 2021 (5 weeks)
	Extra window for catching up on the delayed work and polishing the work done	23th Mar, 2021 to 20th Apr, 2021 (4 weeks)